Software Assurance

The Department of Homeland Security's Software Assurance Program seeks to reduce software vulnerabilities, minimize exploitation, and address ways to improve the routine development and deployment of trustworthy software products. Together, these activities will enable more secure and reliable software that supports mission requirements across enterprises and the critical infrastructure. Because software is essential to the operation of the Nation's critical infrastructure and it is estimated that 90 percent of reported security incidents result from exploits against defects in the design or code of software, ensuring the integrity of software is key to protecting the infrastructure from threats and vulnerabilities, and reducing overall risk to cyber attacks.

Setting a Higher Standard for Software Assurance

The Department's cyber security division's Software Assurance Program partners with the private sector, academia, and other federal departments and agencies to improve software development, quality assurance, and acquisition processes. This effort will lead to the production of higher quality, more secure software in support of government and private-sector mission assurance. Significant new research on secure software engineering is underway, examining a range of development issues from new methods that avoid basic programming errors, to enterprise systems that remain secure when portions of the system software are compromised.

Key Objectives – From Patch Management to Software Assurance

The Software Assurance Program is a strategic initiative grounded in the National Strategy to Secure Cyberspace issued by President Bush in February 2003. A key objective is to shift the security paradigm from patch management to software assurance. This shift is designed to encourage software developers to raise overall software quality and security from the start, rather than relying on applying patches to systems after vulnerabilities are discovered. The Software Assurance Program is designed to spearhead the development of practical guidance and tools and to promote research and development investment in cyber security. The goal is to enable more secure and reliable software that supports mission requirements across enterprises and the infrastructure.

Building Success Through Collaboration

Public-private partnerships form the foundation of the Software Assurance Program. Through Homeland Security's sponsorship of conferences and workshops, a common body of knowledge and a repository of practical guidance for software developers and architects are being produced to improve the quality, reliability, and dependability of software. In collaboration with industry, academia, and government partners, Homeland Security's approach to addressing software assurance encompasses the following components:

- People[1] – Education and training for developers and users.
- Processes[2] – Practical guidelines and best practices for the development of secure software.
- Technology[3] – Tools for evaluating software vulnerabilities and quality.
- Acquisition[4] – Specifications and guidelines for acquisition and outsourcing.

Obtaining Additional Information

To learn more about Homeland Security's Software Assurance Program, visit us at:

https://buildsecurityin.us-cert.gov/swa/[5]

Cyber security is a shared responsibility. Working together, we can secure America's cyberspace.

[5] https://buildsecurityin.us-cert.gov/swa/index.html